CVE-2026-0300 PAN-OS: Unauthenticated user initiated Buffer Overflow Vulnerability in User-ID™ Authentication Portal

Urgency HIGHEST

Severity 9.3 · CRITICAL

Exploit Maturity **ATTACKED**	Response Effort **MODERATE**	Recovery **USER**	Value Density **CONCENTRATED**
Attack Vector **NETWORK**	Attack Complexity **LOW**	Attack Requirements **NONE**	Automatable **YES**
User Interaction **NONE**	Product Confidentiality **HIGH**	Product Integrity **HIGH**	Product Availability **HIGH**
Privileges Required **NONE**	Subsequent Confidentiality **LOW**	Subsequent Integrity **LOW**	Subsequent Availability **NONE**

CVE JSON CSAF

Published **2026-05-05**

Updated **2026-05-06**

Discovered **in production use**

Description

A buffer overflow vulnerability in the User-ID™ Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN-OS software allows an unauthenticated attacker to execute arbitrary code with root privileges on the PA-Series and VM-Series firewalls by sending specially crafted packets.

The risk of this issue is greatly reduced if you secure access to the User-ID™ Authentication Portal per the best practice guidelines by restricting access to only trusted internal IP addresses.

Prisma Access, Cloud NGFW and Panorama appliances are not impacted by this vulnerability.

Product Status

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h5 < 12.1.7	>= 12.1.4-h5 (ETA: 05/13) >= 12.1.7 (ETA: 05/28)

PAN-OS 11.2	< 11.2.4-h17 < 11.2.7-h13 < 11.2.10-h6 < 11.2.12	>= 11.2.4-h17 (ETA: 05/28) >= 11.2.7-h13 (ETA: 05/13) >= 11.2.10-h6 (ETA: 05/13) >= 11.2.12 (ETA: 05/28)
PAN-OS 11.1	< 11.1.4-h33 < 11.1.6-h32 < 11.1.7-h6 < 11.1.10-h25 < 11.1.13-h5 < 11.1.15	>= 11.1.4-h33 (ETA: 05/13) >= 11.1.6-h32 (ETA: 05/13) >= 11.1.7-h6 (ETA: 05/28) >= 11.1.10-h25 (ETA: 05/13) >= 11.1.13-h5 (ETA: 05/13) >= 11.1.15 (ETA: 05/28)
PAN-OS 10.2	< 10.2.7-h34 < 10.2.10-h36 < 10.2.13-h21 < 10.2.16-h7 < 10.2.18-h6	>= 10.2.7-h34 (ETA: 05/28) >= 10.2.10-h36 (ETA: 05/13) >= 10.2.13-h21 (ETA: 05/28) >= 10.2.16-h7 (ETA: 05/28) >= 10.2.18-h6 (ETA: 05/13)
Prisma Access	None	All

Required Configuration for Exposure

This issue is applicable only to PA-Series and VM-Series firewalls that are configured to use User-ID™ Authentication Portal.

Customers are impacted if both of the following conditions are true:

- User-ID™ Authentication Portal configured in the User-ID™ Authentication Portal Settings page. You can verify the configuration by going to Device > User Identification > Authentication Portal Settings -> Enable Authentication Portal (applies to both transparent and redirect modes) **and**
- An interface management profile with response pages enabled and associated with an external/internet-accessible interface. You can verify the configuration by going to Network > Interface > Select the interface > Advanced Tab > Create Management Interface Profile.

Severity: CRITICAL, Suggested Urgency: HIGHEST

The risk is highest when you configure the User-ID™ Authentication Portal to enable access from the Internet or any untrusted network.
CRITICAL - CVSS-BT: 9.3 /CVSS-B: 9.3
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:A/AU:Y/R:U/V:C/RE:M/U:Red)

You can greatly reduce the risk of exploitation by restricting User-ID™ Authentication Portal access to only trusted internal IP addresses and preventing its exposure to the internet.
HIGH - CVSS-BT: 8.7 /CVSS-B: 8.7
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:A/AU:Y/R:U/V:C/RE:M/U:Red)

Exploitation Status

Limited exploitation has been observed targeting Palo Alto Networks User-ID™ Authentication Portals that are exposed to untrusted IP addresses and/or the public internet. Customers following standard security best practices, such as restricting sensitive portals to trusted internal networks are at a greatly reduced risk.

Weakness Type and Impact

CWE-787: Out-of-bounds Write

CAPEC-100 Overflow Buffers

Solution

This issue will be fixed in upcoming releases of PAN-OS as captured in the table above.

We strongly recommend that you secure access to your User-ID™ Authentication Portal following the instructions in the workarounds section below.

Workarounds and Mitigations

Customers can mitigate the risk of this issue by taking either of the following actions:

- Restrict User-ID™ Authentication Portal access to only trusted zones and in addition, disable Response Pages in the Interface Management Profile attached to every L3 interface in any zone where untrusted/internet traffic can ingress. Keep Response Pages enabled only on interfaces in trust/internal zones where legitimate users' browsers ingress. Refer to Step 6 of the following Live Community article and Knowledgebase article for steps to restrict access.
- Disable User-ID™ Authentication Portal if not required.

Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510019 from Applications and Threats content version 9097-10022. Decoder capabilities necessitate PAN-OS 11.1 or a later version for Threat ID support.

CPEs

cpe:2.3:o:palo_alto_networks:pan-os:12.1.6:*:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:12.1.5:*:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:12.1.4:h3:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:12.1.4:h2:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:12.1.4:-:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:12.1.3:*:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:12.1.2:*:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:11.2.11:*:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:11.2.10:h4:*:*:*:*:*:*

cpe:2.3:o:palo_alto_networks:pan-os:11.2.10:h3:*:*:*:*:*:*

Show More

CPE Applicability

- cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)12.1.4 **and** up to (excluding)12.1.4-h5
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)12.1.0 **and** up to (excluding)12.1.7
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.2.4 **and** up to (excluding)11.2.4-h17
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.2.7 **and** up to (excluding)11.2.7-h13
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.2.10 **and** up to (excluding)11.2.10-h6
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.2.0 **and** up to (excluding)11.2.12
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.4 **and** up to (excluding)11.1.4-h33
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.6 **and** up to (excluding)11.1.6-h32
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.7 **and** up to (excluding)11.1.7-h6
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.10 **and** up to (excluding)11.1.10-h25
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.13 **and** up to (excluding)11.1.13-h5
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)11.1.0 **and** up to (excluding)11.1.15
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.2.7 **and** up to (excluding)10.2.7-h34
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.2.10 **and** up to (excluding)10.2.10-h36
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.2.13 **and** up to (excluding)10.2.13-h21
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.2.16 **and** up to (excluding)10.2.16-h7
- **OR**cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* **is vulnerable** from (including)10.2.18 **and** up to (excluding)10.2.18-h6

Timeline

2026-05-06 Updated with Threat Prevention ID and clarified the Required Configuration section.

2026-05-05 Initial publication.